PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-349851
(43)Date of publication of application : 15.12.2000

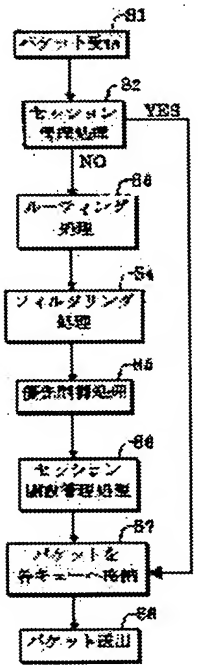
(51)Int.Cl. H04L 29/06
H04L 12/56

(21)Application number : 11-155411
(22)Date of filing : 02.06.1999

(71)Applicant : FUJITSU LTD
(72)Inventor : KOJIMA YUJI
TSURUOKA TETSUAKI

(54) DEVICE FOR PACKET TRANSFER

(57)Abstract:
PROBLEM TO BE SOLVED: To enable security control and priority transfer control corresponding to a session by giving a subsequent packet belonging to the same session to the bypass path of a main processing part based on the packet information.
SOLUTION: When a received packet (S1) is managed as a session (S2), the packet is directly transferred to a switching part and a packet scheduling processing part (S7) without performing routing processing (S3), filtering processing (S4) nor priority control processing (S5), is transmitted (S8) and transferred without performing redundant processing. Information (packet information) for identifying a specified packet is defined by detecting the session in this way, the hardware part of a packet transferring device processes security control and priority transfer control to be executed based on the definition information while cooperating with a main processing part, and about a packet capable of being analogized from a previously arriving packet, the packet is transmitted by bypassing the main processing part.



LEGAL STATUS

[Date of request for examination]	19.06.2001
[Date of sending the examiner's decision of rejection]	
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	3403971
[Date of registration]	28.02.2003
[Number of appeal against examiner's decision of rejection]	

[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－349851
（P2000－349851A）
(43)公開日　平成12年12月15日(2000.12.15)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'（参考）
Ｈ０４Ｌ　29/06		Ｈ０４Ｌ　13/00	３０５Ｄ	５Ｋ０３０
12/56		11/20	１０２Ａ	５Ｋ０３４
				９Ａ００１

審査請求　未請求　請求項の数12　ＯＬ　（全 21 頁）

(21)出願番号　特願平11－155411

(22)出願日　平成11年６月２日(1999.6.2)

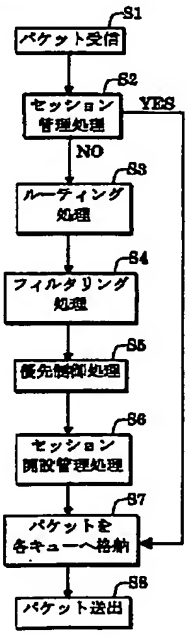
(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号
(72)発明者　小島　祐治
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(72)発明者　鶴岡　哲明
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(74)代理人　100090011
弁理士　茂泉　修司

最終頁に続く

(54)【発明の名称】　パケット転送装置

(57)【要約】
【課題】各ネットワークに属する端末間の通信を行うパケット転送装置において、セッションに対応したセキュリティ制御及び優先制御を可能にする。
【解決手段】ルーティング処理、フィルタリング処理、及び優先制御処理を実行する主処理部から出力されたパケットがセッション開設条件に適合するか否かを判定し、該パケットについて適合判定した時、そのパケット情報を保持し、該パケット情報に基づいて同一セッションに属する後続のパケットを、該主処理部をバイパスして送出する。

パケット転送装置の各処理間のフローチャート



【特許請求の範囲】
【請求項１】各ネットワークに属する端末間の通信を行うパケット転送装置において、
ルーティング処理、フィルタリング処理、及び優先制御処理を実行する主処理部と、
該主処理部から出力されたパケットがセッション開設条件に適合するか否かを判定するセッション開設判定部と、
該セッション開設判定部が該パケットについて適合判定した時、該判定部からそのパケット情報を受けて保持し、該パケット情報に基づいて同一セッションに属する後続のパケットを該主処理部のバイパス路に与えるセッション管理判定部と、
を備えたことを特徴とするパケット転送装置。
【請求項２】請求項１において、
該セッション開設判定部が、ネットワーク管理方針に従って予めパケット情報と優先情報とが設定されたセッション開設管理テーブルと、該テーブルを検索してセッション開設条件の適合の有無を判定するセッション開設管理処理部と、で構成されていることを特徴としたパケット転送装置。
【請求項３】請求項２において、
該セッション管理判定部が、該セッション開設管理処理部から与えられる同一セッションに関する該パケット情報を動的に保持するセッション管理テーブルと、該セッション管理テーブルを検索して同一セッションの後続パケットを該バイパスに与えるセッション管理処理部と、で構成されていることを特徴としたパケット転送装置。
【請求項４】請求項３において、
該セッション管理判定部が、該セッション管理テーブルを検索して適合するエントリがないときは、各エントリの構成情報を反転して再度検索を行うことを特徴としたパケット転送装置。
【請求項５】請求項３において、
通信形態がＴＣＰ通信のとき、パケットフォーマットのコードビットを用いて該セッションの開設又は閉鎖を行うことを特徴としたパケット転送装置。
【請求項６】請求項５において、
該セッション管理判定部が、該コードビットのＦＩＮをセッション閉鎖フラグとして用い、このフラグが設定されたパケットを受信し、さらに後続の閉鎖受信応答パケットを該セッション管理処理部が受信したとき該セッションの閉鎖を行うとともに該セッション管理テーブルの適合するエントリを削除することを特徴としたパケット転送装置。
【請求項７】請求項５において、
該セッション管理判定部が、該コードビットのＲＳＴをセッション閉鎖フラグとして用い、このフラグが設定されたパケットを受信したとき、以後、該セッションの閉鎖を行うとともに該セッション管理テーブルの適合するエントリを削除することを特徴としたパケット転送装置。
【請求項８】請求項５において、
該セッション管理判定部が、一定時間以上パケットの送受信が無いとき、以後、該セッションの閉鎖を行うとともに該セッション管理テーブルの適合するエントリを削除することを特徴としたパケット転送装置。
【請求項９】請求項５において、
通信形態がＵＤＰ通信のとき、該セッション開設管理テーブルが、ＵＤＰパケットヘッダに続くアプリケーションデータ部の一部のビットパターンを保持するＵＤＰセッション開設データ・テーブルを含み、該セッション開設管理処理部が、該セッション開設管理テーブルと該ＵＤＰセッション開設データ・テーブルを検索してセッションの開設を行うことを特徴としたパケット転送装置。
【請求項10】請求項９において、
該セッション管理判定部が、一定時間以上パケットの送受信が無いとき、以後、該セッションの閉鎖を行うとともに該セッション管理テーブルの適合するエントリを削除することを特徴としたパケット転送装置。
【請求項11】請求項9において、
各テーブルにマスクデータ・テーブルが付設されていることを特徴としたパケット転送装置。
【請求項12】請求項３において、
該セッション管理テーブルが、各フィールド値の必要な種類数分のインデックス付けを行い、該インデックスの組み合わせにより、該テーブルを構成することを特徴としたパケット転送装置。
【発明の詳細な説明】
【０００１】
【発明が属する技術分野】本発明は、パケット転送装置に関し、特にTCP通信又はUDP通信により端末が接続されているネットワークにおいて、パケット転送を実行するパケット転送装置に関するものである。
【０００２】端末間の通信のためのネットワークの利用の拡大に伴い、ネットワークの規模拡大のためにネットワーク間の中継、例えばLAN(Local Area Network)とLAN、又はLANと専用線を相互接続する必要が生じる。こうして構築されるネットワークで現在主流なのはIP(Internet Protocol)によるネットワークである。このIPは、ISO(International Organization for Standardization)のOSI(Open Systems Interconnection)モデルにおけるネットワーク層に相当するコネクションレス型のプロトコルである。
【０００３】コネクションレス型のIP通信では、予め端末間で通信路を確保するコネクション型のプロトコルと異なり、LAN間を相互接続するパケット転送装置が、通信データを格納しているパケットを転送処理することによって端末間の通信が実現する。
【０００４】このコネクションレス型のIP通信を用い

て、コネクション型の通信を実現するためには、より上位のトランスポート層及びセッション層に相当するTCP(Transmission Control Protocol)によって、「セッション」と呼ばれるコネクションを確立してから、端末間で通信を行う必要がある。

【０００５】一方、端末間でコネクションレス型のパケット通信を行うときには、TCPの代わりにコネクションレス型のUDP(User Datagram Protocol)を用いる。このTCP及びUDPのどちらを用いて通信を行うかは、端末間で通信を行う個別のアプリケーションが選択することになる。

【０００６】

【従来の技術】図10は、複数のLANをパケット転送装置が相互接続しているときの一般的なネットワーク構成例を示している。この構成例において、同一のLANに接続されている端末同士は、パケット転送装置を介さずに直接相互に通信する。例えばLAN1に接続されている端末11と端末13は、LAN1を介してパケットを送受信することによって直接通信することができる。

【０００７】一方、同一のLANに接続されていない端末同士は、複数のパケット転送装置及び複数のLANを介して通信する。例えば、端末11と端末62との間の通信は、端末11が送信したパケットが、LAN1→パケット転送装置1→LAN4→パケット転送装置2→LAN5→パケット転送装置3→LAN6の順に中継されて端末62で受信し、さらに、端末62から送信されたパケットは上記と逆方向に中継され、端末11が受信することによって実現する。

【０００８】このときパケット転送装置1は、LAN1に接続されているインタフェースIF1で端末11が送信したパケットを受信し、パケット内において宛先アドレス等のそのパケットの制御情報が格納されているヘッダ部の各フィールド値から、そのパケットを送出すべきインタフェースとしてLAN4に接続されているインタフェースIF4を決定し、このインタフェースIF4から該パケットを送出する。同様にインタフェースIF4は、端末62から送信されたパケットを受信し、インタフェースIF1から該パケットをLAN1に送出するというパケット転送処理を行う。

【０００９】このようなパケット転送処理を、個々のパケット転送装置(例えば図10のネットワーク構成例では、パケット転送装置1、パケット転送装置2、及びパケット転送装置3)が実行することによって、端末間の通信が実現する。一方、パケット転送装置は、パケットを転送するだけでなく、ある特定のパケットを転送せずに廃棄することによって、ネットワーク管理の一環としてネットワーク上で特定の通信を禁止し、不正なアクセスを防ぐことも一般的な機能として持っている。

【００１０】特定の端末、特定の端末群、特定のLAN、及び特定のアプリケーション間の通信を許可／禁止することは、パケット転送装置が特定のパケットを転送／廃棄するための、「フィルタリング処理」を行うことによって可能となる。例えば、図10のネットワーク構成例において、LAN2に接続されている端末22とLAN1に接続されている端末群との通信に関して、端末22－端末11間の通信は許可し、それ以外の端末22－端末12間及び端末22－端末13間の通信は禁止するというネットワーク管理をネットワーク管理者が行う場合、パケット転送装置1は、送信元アドレスが端末22を指し示しており、かつ宛先アドレスが端末11を指し示しているパケットと、送信元アドレスが端末11を指し示しており、かつ宛先アドレスが端末22を指し示しているパケットのみを転送する。

【００１１】上記の条件を満たさず、かつ送信元アドレスが端末22を指し示しており、かつ宛先アドレスの上位ビットがLAN1に接続されている端末を指し示しているときはパケットを廃棄するというフィルタリング処理を実行する。一般に、IPネットワークにおいては、同一LANに接続している端末は、同一のサブネットワークに属しており、各端末のアドレスは、ある一定範囲のその上位ビットが等しくなる。上述のフィルタリング処理によって、ネットワーク管理者が、端末22とLAN1に接続されている端末群との通信は端末22－端末11との間を除いて禁止するというネットワーク管理を行うことが可能である。

【００１２】上記の例と同様にパケット単位で転送／廃棄を決定する各種のフィルタリング条件を、ネットワーク管理者が組み合わせてパケット転送装置に設定することによって、例えば、図10におけるLAN1, LAN2, 及びLAN3が社内の内部ネットワークとして、パケット転送装置1のインタフェースIF4を社外との接続点として、必要な通信は許可しつつ、LAN4, LAN5, 及びLAN6のような社外の外部ネットワークからの不正なアクセスを制御するという、より複雑なネットワークのセキュリティ制御をネットワーク管理者は行うことが可能となる。

【００１３】また、ネットワーク上のある特定の通信を、単に許可/禁止するだけではなく、他の通信よりも優先的に扱うといった「優先制御」は、パケット転送装置が特定の通信のパケットを判別し、判別した該パケットを優先的に処理することによって実現する。

【００１４】この優先制御処理は、パケット転送装置が特定のパケットを判別するという点においてはフィルタリング処理と同じ処理であり、フィルタリング処理と優先制御処理との違いは、パケット転送装置が、パケット判別後に、該パケットを転送/廃棄するか、該パケットを優先するかの違いである。

【００１５】例えば、図10のネットワーク構成例において、他の端末へ重要なサービスを提供するサーバである端末31と他の端末との通信においては、他の通信よりも優先的に処理するというネットワーク管理をネットワーク管理者が行う場合、パケット転送装置1は、パケットのヘッダの宛先アドレスまたは送信元アドレスが端末31

を指し示すときは、高い優先度でパケットを転送するように、パケット転送装置1に設定する。このような優先制御処理をパケット転送装置1が実行することによって、端末31と他の端末との通信の優先制御を行うことが可能となる。

【００１６】上述したセキュリティ制御及び優先制御を、従来のパケット転送装置は、図11で示す処理構成で実行する。例えば、パケット転送装置100（これは上記の装置1～3を総称している）が、セキュリティ制御を行うとき、ネットワーク管理者は、ソフトウエア部101を構成するセキュリティ制御ソフトウェア102に対しネットワークの管理方針に基づき予め設定を行う。

【００１７】そして、その設定を、ハードウェア部104にあるフィルタリングテーブル108の各フィルタリングエントリに適合する形へ、セキュリティ制御ソフトウェア102が変換する。セキュリティ制御ソフトウェア102は、変換した各エントリをフィルタリングテーブル108へ格納するように、ハードウエア部104中のフィルタリング処理部109へ依頼する。

【００１８】フィルタリング処理部109はセキュリティ制御ソフトウェア102から依頼された各エントリをフィルタリングテーブル108へ格納する。このような手順で、パケット転送装置100は、予めフィルタリングテーブル108へ各フィルタリングエントリを格納しておく。そして、フィルタリング処理部109が、受信したパケットとフィルタリングテーブル108の各エントリを各フィールド値により比較して、その受信したパケットに対し該当するエントリが存在したならば、該当するエントリ内の「転送/廃棄フィールド」の値（例えば、転送なら‘1’、廃棄なら‘0’）に従って受信パケットを転送または廃棄する。

【００１９】また同様に、パケット転送装置100が優先制御を行うとき、ネットワーク管理者が、ソフトウェア部101を構成する優先制御ソフトウェア103に対しネットワークの管理方針に基づいて予め設定を行う。そして、その設定を、ハードウェア部104にある優先制御テーブル110の各エントリに適合する形へ、優先制御ソフトウエア103が変換する。

【００２０】優先制御ソフトウエア103は、変換した各エントリを優先制御テーブル110へ格納するように、ハードウエア部104中の優先制御処理部111へ依頼する。優先制御処理部111は、優先制御ソフトウエア103から依頼された各エントリを優先制御テーブル110へ格納する。

【００２１】このような手順で、パケット転送装置100は、予め優先制御テーブル110へ各優先制御エントリを格納しておく。そして、優先制御処理部111が、受信したパケットと優先制御テーブル110の各エントリとを各フィールド値により比較して、その受信したパケットに対し該当するエントリが存在したならば、その該当するエントリ内の「優先度フィールド」の値（例えば‘0’～‘7’）に従って、パケット転送装置100が、その受信パケットを優先的に転送する。

【００２２】また、上述のフィルタリング処理部109及び優先制御処理部111は、パケットの送出インタフェースに基づき、フィルタリングテーブル108及び優先制御テーブル110を検索するので、フィルタリング処理部109及び優先制御処理部111より前段にルーティング処理部107及びルーティングテーブル106を配置している。

【００２３】なお、フィルタリング処理部109で廃棄と決定されるであろうパケットに関して、優先制御処理部111が処理を行っても無駄であるので、一般に優先制御処理部111の前段にフィルタリング処理部109を配置している。以下に、受信パケットに対して図12に示したパケット転送装置100が行う一連の転送処理動作として、上述の個々の処理部を説明する。

【００２４】受信インタフェースにパケットが到着すると、ルーティング処理部107が宛先アドレス(例えば、IP通信ならば宛先IPアドレス)に基づいてルーティングテーブル106を検索し、受信パケットを送出するインタフェース及びそのときの送出パケットのMAC(Media Access Control)アドレスを決定する。

【００２５】次に、ルーティング処理部107は、受信パケットを次処理部であるフィルタリング処理部109へ送出するとともに、上述のルーティング処理部107が決定した送出インタフェース及びMACアドレスをフィルタリング処理部109へ通知する。ここで、MACアドレスとは、LANに接続されている中継装置（図示せず）又は端末のインタフェースを識別するアドレスであり、同一のLANに接続されている端末／中継装置同士が通信するために必要なアドレスである。

【００２６】ルーティングテーブル106には、予め宛先IPアドレスに対する送出インタフェースとMACアドレスの対応関係を、ネットワーク管理者が入力するか、装置制御ソフトウェアが隣接する中継装置と通信することによって格納する。また、上述のルーティング処理部107が決定した送出インタフェース番号及びMACアドレスをフィルタリング処理部109へ通知するといったように、パケットとともにそのパケットに付随する情報を次処理部へ通知する方法としては、例えばパケットヘッダ（図13により後述する）の更に前に装置内制御用ヘッダを前処理部で付加し、その装置内制御用ヘッダの特定のフィールドへ、次処理部へ通知する情報を前処理部が格納すればよい。

【００２７】ルーティング処理部107からパケットを受信したフィルタリング処理部109は、パケットヘッダ内の各フィールド値及び受信したパケットの送信／受信インタフェースに基づき、フィルタリングテーブル108を検索し、受信したパケットが廃棄のフィルタリング条件と合致したならば廃棄し、それ以外ならば受信したパケットを次処理部である優先制御処理部111へ渡す。

【００２８】優先制御処理部111は、パケットヘッダ内の各フィールド値及び受信したパケットの送信／受信インタフェース番号に基づいて優先制御テーブル110を検索し、ある特定のエントリに受信したパケットが適合するならば、同エントリに格納した優先度及びパケットを、次処理部であるスイッチ部112へ渡す。

【００２９】スイッチ部112は、受信したパケットを、パケットの送出インタフェース番号及び優先度に応じてパケットスケジューリング処理部114内の各送出キュー113へ格納する。例えば、パケットスケジューリング処理部114には、図示の如く、各送出インタフェース115毎に3つのキューを用意して、パケット転送装置100が「0～7」の8段階の優先度を有するようにするならば、「0～2」が低優先のキュー、「3～5」が中優先のキュー、「6～7」が高優先のキューといったように割り振る。

【００３０】パケットスケジューリング処理部114は各キューからパケットをパケットスケジューリング方法に従って取り出し、送出インタフェース115へ送出する。上述のパケットスケジューリング方法としては、例えば単純なものとして、より高い優先度を持つパケットを格納するキュー113から先にパケットを送出し、より高い優先度のキュー内が空であったならば、次に高い優先度を持つキュー113からパケットを送出するというような方法がある。

【００３１】このようにパケットの優先度に応じて先にパケットを送出することによって、パケット転送装置100は優先転送制御を行うことができ、最終的に送出インタフェース115からパケットを送出する。ここでフィルタリングテーブル108のテーブル構造について図12及び図13により具体的に説明する。

【００３２】例えばIPの場合、図13に示すIPパケットフォーマットのヘッダ内の各フィールド値（プロトコル番号、送信元IPアドレス、宛先IPアドレス、送信元ポート番号、宛先ポート番号、受信インタフェース番号、及び送信インタフェース番号）に対応してテーブル108は、図12（1）及び（2）にそれぞれ示すように、フィルタリング条件・テーブルとマスクデータ・テーブルとで構成される。

【００３３】フィルタリング条件・テーブルの各エントリは、図示のように、対応するマスクデータ・テーブルの各エントリとポインタによって関係付けられている。フィルタリング条件・テーブルには、パケット転送装置がフィルタリング処理を行うパケットの条件を格納し、マスクデータ・テーブルには、その各フィルタリング条件の各フィールド値が有意な条件かどうかを示す‘0’，‘1’のビット列を格納する。

【００３４】例えば、フィルタリング条件・テーブルのフィルタリング条件301においては、プロトコル番号、送信元IPアドレス、及び宛先IPアドレスの3つの条件を設定し、他の送信元ポート番号、宛先ポート番号、受信インタフェース番号、及び送出インタフェース番号は設定していない。

【００３５】したがって、フィルタリング条件301に対応するマスクデータ306に関して、送信元ポート番号、宛先ポート番号、受信インタフェース番号、及び送出インタフェース番号のフィールド値をビット列として「00…0」に設定する。さらに、送信元IPアドレスに関して、フィルタリング条件301では、「150.56.0.0」（これは、ビット列10010110 00111000 00000000 00000000と等しい）になっているが、対応するマスクデータ306の送信元IPアドレスが「255.255.0.0」（これは、ビット列11111111 11111111 00000000 00000000と等しい）になっている。

【００３６】従って、送信元IPアドレスが「150.56.0.0」であるパケットのみが、フィルタリング条件301の送信元IPアドレスに適合するのではなく、送信元IPアドレスが「150.56.(0～255).(0～255)」であるパケットの全てが、フィルタリング条件301の送信元IPアドレスの条件に適合する。

【００３７】同様に宛先IPアドレスに関しても、フィルタリング条件301では、宛先IPアドレスが「10.(0～255).(0～255).(0～255)」であるパケットの全てが、フィルタリング条件301の宛先IPアドレスの条件に適合する。すなわち、マスクデータテーブルのマスク値は、パケットヘッダ内フィールド値に対し、フィルタリング条件・テーブルの各エントリの各フィールド値が適合する範囲を指定することになる。

【００３８】マスクデータ・テーブルに設定する総エントリ数は、フィルタリング条件・テーブルに設定した総エントリ数と等しい必要は無く、例えば、フィルタリング条件302のマスクデータのパターンは、フィルタリング条件301と等しいので、フィルタリング条件302のポインタはマスクデータ306を指すように設定することにより、フィルタリング条件・テーブルに設定した総エントリ数よりもマスクデータテーブルに設定した総エントリ数の方が少なくて済む。

【００３９】なお、フィルタリング条件・テーブルの「プロトコル番号」を、「TCP」又は「UDP」という文字で表記したが、フィルタリング条件・テーブルをパケット転送装置100のハードウェア部104における記憶デバイス（図示せず）で実装するときは、これを、TCP=0、UDP=1のようにそれぞれ対応するビットで記憶デバイス内に格納することになる。

【００４０】同様に、フィルタリング条件・テーブルの「転送/廃棄」を、「転送」又は「廃棄」という文字で表記したが、フィルタリング条件・テーブルをハードウェア部104における記憶デバイスで実装するときは、これを、転送=0、廃棄=1のようにそれぞれ対応するビットで記憶デバイス内に格納することになる。

【００４１】優先制御テーブル110についても、フィル

タリングテーブル108と同様に、優先制御条件・テーブルとマスクデータ・テーブルを持ち、優先制御条件・テーブル及びマスクデータ・テーブルのフィールドとして、プロトコル番号、送信元IPアドレス、宛先IPアドレス、送信元ポート番号、宛先ポート番号、受信インタフェース番号、及び送出インタフェース番号のフィールドを持ち、フィルタリング条件・テーブルの「転送/廃棄」フィールドが、「優先度」に置き換わったテーブル構造になっている。

【００４２】上述のフィルタリングテーブル108及び優先制御テーブル110をハードウェア部104に実装するときは、一般にCAM(Content Addressable Memory; 連想記憶)という記憶デバイスによって実装する。記憶デバイスとして、このようなCAMを用いることにより、他のメモリ等とは違ってCAMは、メモリ内の各エントリと検索キーであるパケット内フィールド値との比較を1エントリずつ行うのではなく、検索キーと全エントリを並列に同時比較することが可能なので、テーブル内に格納したエントリ数に関係なく高速に受信パケットに対し該当するエントリを検索することができる。

【００４３】

【発明が解決しようとする課題】従来のパケット転送装置のハードウェア部が具備しているフィルタリングテーブル、優先制御テーブル、並びにこれらのテーブルの検索・更新・結果判断を行うフィルタリング処理部及び優先制御処理部は、パケット単位でのエントリ構成を持ち、なおかつパケット転送装置に到着する1つのパケット毎に転送/廃棄、及び優先度を判断していた。

【００４４】したがって、例えば、あるアプリケーションに関する通信において、通常、外部ネットワークから発信が開始された通信は禁止または低優先で扱うが、内部ネットワークから発信が開始された通信に関しては許可または高優先で扱うというような、セッション開設方向に応じたセキュリティ制御及び優先転送制御を行うことができないという問題点があった。これをもう少し具体的に説明する。

【００４５】例えば、図3（１）のTCP通信の場合、パケット①と③は、図12に示したフィルタリング条件では区別することができない。これは、パケット①と③は、いずれも外部ネットワークに属する端末62が発信したパケットであるからである。しかしながら、パケット③は、元々内部ネットワークに属する端末11が発信したパケット②が起因して開始された一連の通信に属しているのに対して、パケット①は、元から外部ネットワークに属する端末62が発信したパケット①に起因した通信である。したがって、パケット①と③を区別して、パケット転送装置は、廃棄/転送しなければならない。

【００４６】これを行うためには、パケット単位ではなく、前のパケット（たとえばパケット②）の属性に基づいて、後のパケット（たとえばパケット③）を識別するための情報を定義する必要がある。そうすることによって、セッション開設方向に応じたセキュリティ制御及び優先転送制御を行うことが可能となる。

【００４７】上述のセッション開設方向に応じたセキュリティ制御及び優先転送制御を行うためには、この処理を行うセキュリティ制御／優先転送処理部をパケット転送装置内に新たに設ければよい。このとき、該セキュリティ／優先転送処理部も、図11に示す順番にパケット転送装置内に配置されたルーティング処理部、フィルタリング処理部、及び優先制御処理部を適切に協業するようにパケット転送装置内に配置する必要がある。

【００４８】これにより、パケット転送装置が実行するパケット転送処理が遅くなることを避け、各処理部で重複している冗長な処理を省き、以って高速パケット転送処理を実現することができる。この場合の適切に協業するとは、例えば、セキュリティ／優先転送処理部が、受信パケットに対し処理を実行することによって、送出インタフェースが判別する場合はルーティング処理を行わないというような、ルーティング処理部と協業を行う場合が挙げられる。

【００４９】従って、従来のパケット転送装置は、セッションを検出することができず、従ってある特定のパケットを識別するための情報を定義し、その定義情報に従ってセキュリティ制御及び優先転送制御が実行できないという問題点があった。また、ルーティングテーブル及びフィルタリングテーブルを検索する必要がないパケットまで冗長に検索してしまいパケット転送処理の高速化にとって不利であるという問題点があった。

【００５０】更に、図11の従来のパケット転送装置が有するフィルタリングテーブル及び優先制御テーブルは、例えばネットワーク管理者が設定に使用するソフトウェアにより、各エントリを各フィールド値の範囲を表現するマスク値とともに格納するので、エントリ数自体は少ないが、上記の問題点を解決するために新たに設けるセッション管理テーブルは、端末間の通信に基づいてエントリを格納するので、セッション管理テーブルの保有エントリ数が多くなり、そのセッション管理テーブルを実装するための使用メモリ容量が膨大になるという問題点もあった。

【００５１】従って、本発明は、セッションに対応したセキュリティ制御及び優先転送制御が可能なパケット転送装置を実現することを課題とする。また、使用メモリ容量を節約することを課題とする。

【００５２】

【課題を解決するための手段】上記の課題を解決するため、本発明に係るパケット転送装置は、概略的には、セッションを検出することによって、ある特定のパケットを識別するための情報を定義し、この定義情報に従って、セキュリティ制御及び優先転送制御(主処理部によるルーティング処理、フィルタ処理、及び優先制御処

理)を実行するとともに、前着しているパケットから類推できる同一セッションのパケットに関しては、主処理部を経由せずにパケットを送出することによって高速にパケット転送を行うとするものである。

【００５３】すなわち、本発明では、パケット転送装置内に、主処理部に加えて、セッション管理判定部を構成するセッション管理処理部及びセッション管理テーブルと、セッション開設判定部を構成するセッション開設管理処理部及びセッション開設管理テーブルとを新たに設ける。

【００５４】そして、図1に示すように、受信したパケット（ステップS1）がセッションとして管理していないパケットであれば、セッション管理処理部（同S2）→ルーティング処理部（同S3）→フィルタリング処理部（同S4）→優先制御処理部（同S5）→セッション開設管理処理部（同S6）→スイッチ部→パケットスケジューリング処理部（同S7）の順に処理して送出インタフェースから送出する（同S8）。

【００５５】一方、受信パケット（同S1）がセッションとして管理しているパケットであれば（同S2）、ルーティング処理（同S3）、フィルタリング処理（同S4）、及び優先制御処理（同S5）を行わずにスイッチ部及びパケットスケジューリング処理部に直接渡し（同S7）、パケットを送出（同S8）して、上記冗長な処理をせず、高速にパケットを転送している。

【００５６】セッション開設管理処理部は、主処理部を構成する優先制御処理部の後段に配し、上述したようにセキュリティ制御ソフトウェアまたは優先制御ソフトウエア等からの制御により、セッション開設管理テーブルへセッションを開設すべきパケットが識別可能なエントリを格納/更新/削除する。

【００５７】セッション開設管理処理部は、主処理部からパケットを受け取った後、セッション開設管理テーブルを検索し、セッション開設管理テーブルに適合するエントリがあったならば、同一のセッションで該パケットに続く後続のパケットを、パケット情報（そのヘッダから識別可能なフィールドと、後段の主処理部によるルーティン処理、フィルタリング処理、及び優先制御処理を行わずに該パケットを転送可能なように各処理の結果得られた情報を格納したフィールドとを有するエントリ）をセッション管理テーブルへ格納するようにセッション管理処理部へ依頼する。

【００５８】セッション管理処理部は、主処理部を構成するルーティング処理部の前段に配置され、上記の依頼に基づいてセッション管理テーブルへパケット情報（エントリ）を格納する。セッション管理処理部は、パケットを受け取った後、そのパケット情報（パケットヘッダの各フィールド値）を基にセッション管理テーブルを検索し、適合するエントリがあったならば、（該エントリのタイムスタンプを更新し）該エントリに格納されているパケット情報（受信/送出インタフェース番号及び優先度及び宛先物理アドレス(宛先MACアドレス)）をスイッチ部へ通知し、該パケットは主処理部を通らずにバイパスしてスイッチ部へ送られる。

【００５９】セッション管理処理部は、パケットがセッション管理テーブルのエントリに適合し、かつ、セッション閉鎖開始のパケットである旨のフラグが立っていたならば、それを該エントリに記憶しておき、後続の閉鎖受信応答パケットによってセッションが閉鎖されたなら、該エントリをセッション管理テーブルより削除するというセッション閉鎖時の処理を行う。

【００６０】なおセッション管理処理部は、受け取ったパケットが、いかなるセッション管理テーブルのエントリにも適合しない場合、従来と同様にパケットをルーティング処理部へ渡す。このように本発明では、セッション管理処理部、セッション管理テーブル、セッション開設管理処理部、及びセッション開設管理テーブルをパケット転送装置の適切な処理段に配置し、セッションを検出することによって、ある特定のパケットを識別するための情報（パケット情報）が定義され、その定義情報に基づき実行されるセキュリティ制御及び優先転送制御を、主処理部と協業しつつ、パケット転送装置のハードウェア部で処理するとともに、前着しているパケットより類推できるパケットに関しては、主処理部をバイパスしてパケットを送出することにより、高速にパケット転送を行うという課題を解決している。

【００６１】また、使用メモリ容量を節約するため、エントリ内の各フィールド値の中で例えばIPアドレス及びポート番号は、その全番号空間と比較して、実際のネットワーク運用状況においてパケット転送装置を介在して使用される番号空間は少ないので、そのような場合、各フィールド値の必要なパターン数分のインデックス付けをし、該インデックスの組み合わせにより、テーブルを構成すればよい。

【００６２】なお、上記のセッション管理判定部は、該セッション管理テーブルを検索して適合するエントリがないときは、各エントリの構成情報を反転して再度検索を行うことができる。また、通信形態がＴＣＰ通信のとき、パケットフォーマットのコードビットを用いて該セッションの開設又は閉鎖(の判定)を行うことが可能である。

【００６３】例えば、該セッション管理判定部が、該コードビットのＦＩＮをセッション閉鎖フラグとして用い、このフラグが設定されたパケットを受信し、さらに後続の閉鎖受信応答パケットを該セッション管理処理部が受信したとき該セッションの閉鎖(の判定)を行うとともに該セッション管理テーブルの適合するエントリを削除することができる。

【００６４】さらに、該セッション管理判定部が、該コードビットのＲＳＴをセッション閉鎖フラグとして用

い、このフラグが設定されたパケットを受信したとき、以後、該セッションの閉鎖(の判定)を行うとともに該セッション管理テーブルの適合するエントリを削除することもできる。

【００６５】さらに、上記のセッション閉鎖以外に、該セッション管理判定部が、一定時間以上パケットの送受信が無いとき、以後、該セッションの閉鎖(の判定)を行うとともに該セッション管理テーブルの適合するエントリを削除してもよい。一方、通信形態がＵＤＰ通信のとき、該セッション開設管理テーブルが、ＵＤＰパケットヘッダに続くアプリケーションデータ部の一部のビットパターンを保持するＵＤＰセッション開設データ・テーブルを含み、該セッション開設管理処理部が、該セッション開設管理テーブルと該ＵＤＰセッション開設データ・テーブルを検索してセッションの開設(の判定)を行うことが可能である。

【００６６】この場合も、該セッション管理判定部が、一定時間以上パケットの送受信が無いとき、以後、該セッションの閉鎖(の判定)を行うとともに該セッション管理テーブルの適合するエントリを削除してよい。また、各テーブルにマスクデータ・テーブルを付設することができる。

【００６７】

【発明の実施の形態】図2は、本発明に係るパケット転送装置100の一実施例を示している。この実施例では、図11に示したパケット転送装置100において、受信インタフェース105とをルーティング処理部107との間に、セッション管理テーブル121を備えたセッション管理処理部122を設け、優先制御処理部111とスイッチ部112との間にセッション開設管理テーブル123を備えたセッション開設管理処理部124を設けている。そして、処理部122と124とを信号線125で直接接続するとともに処理部122からデータ線126を介して直接パケットをスイッチ部112に送るようにしている。

【００６８】このようなパケット転送装置100は、例えば図10に示した一般的なネットワーク構成例において、LAN1に属する端末群がLAN6に属する端末群へTCPのアプリケーションの一つであるtelnet通信で送信するパケットは、高優先で扱い、LAN6に属する端末群がLAN1に属する端末群へTCP通信で送信しようとするパケットに関しては通信を許可しない、というようなセキュリティ制御及び優先転送制御を行うものである。

【００６９】今、LAN1のIPネットワークアドレスを192.168.10.0(ネットマスク =255.255.255.0)とし、LAN6のIPネットワークアドレスを192.168.60.0(ネットマスク = 255.255.255.0)とし、端末11のIPアドレスを192.168.10.1とし、端末62のIPアドレスを192.168.60.2とする。

【００７０】なお、本実施例においては、図10中のパケット転送装置1～３と図2中のパケット転送装置100と図3及び図4中のパケット転送装置100は、実質的に同一の装置を指すものとする。また、図5は、図2のパケット転送装置100内に設けたセッション開設管理テーブル123を示し、図6は、セッション管理テーブル121を示す。

【００７１】さらに、図3(1)は、TCPのセッション開設時のパケットのフローを示しており、LAN1に属する端末11とLAN6に属する端末62がtelnet通信する例を示している。例えば、パケット転送装置100は、端末62を送信元とするパケット①を転送せずに廃棄したことを示しており、一方、パケット③は転送したことを示している。

【００７２】以下に図3(1)の時間の流れに沿って、TCP通信のセッション開設時に関して図２に示したパケット転送装置が実行する処理を説明する。端末11－端末62間のTCP通信においては、端末62が発信したパケット①がパケット転送装置100に到着したとき、この通信はLAN6に属する端末群がLAN1に属する端末群へ発信したTCP通信であるので、パケット転送装置100は、上記のとおりパケット①を廃棄する。

【００７３】これを実行するため、ネットワーク管理者は、「LAN6に属する端末群がLAN1に属する端末群へ発信したTCP通信は許可しない。」というネットワーク管理方針に従って、セキュリティ制御ソフトウェア102を介してフィルタリングテーブル108へ、図12に示したフィルタリング条件305及び対応マスクデータ309に示すように、プロトコル番号がTCPであり、送信元IPアドレスが192.168.60.0(マスク値255.255.255.0)であり、宛先IPアドレスが192.168.10.0(マスク値255.255.255.0)であり、かつ「転送/廃棄」フィールドの値が廃棄であるエントリを予め格納しておく。

【００７４】このエントリにパケット①が適合（ヒット）することを、従来例で述べたようにようにフィルタリング処理部109が判断して廃棄する。telnet通信を開くパケット②がパケット転送装置100に到着したとき、この通信はLAN1に属する端末群がLAN6に属する端末群へ発信したtelnet通信であるので、パケット②を発信源パケットとするパケット③、④等を、パケット転送装置100は高優先で転送処理する。

【００７５】すなわち、これを実行するため、ネットワーク管理者は、「LAN1に属する端末群がLAN6に属する端末群へ発信したtelnet通信を高優先で転送処理する。」というネットワーク管理方針に従って、優先制御ソフトウエア103を介してセッション開設管理テーブル123へ、図５に示す如く、セッション開設条件801及び対応マスクデータ802のように、プロトコル番号がTCPであり、送信元IPアドレスが192.168.10.0(マスク値255.255.255.0)であり、宛先IPアドレスが192.168.60.0(マスク値255.255.255.0)であり、宛先ポート番号が23(telnet通信であることを示す)であり、かつ「優先度/転送」フィールドが7(高優先)であるエントリを予め格納しておく。

【００７６】一方、TCP通信のセッションを開設するまでの、セッション開設開始のパケットには、TCP通信の

仕様上、図13に示したTCPパケットフォーマットのコードビット(別名; CTR(control)フラグ)のSYNビットが立っている(以降、CTR=SYNと表現する)。セッション開設管理処理部124は、このコードビットをトリガにしてセッション開設管理テーブル123を検索し、パケット②がセッション開設条件801及び対応マスクデータ802のエントリに適合（ヒット）しているか否かを判別する。

【００７７】上記の手順は、図７に示すセッション開設管理処理部124のステップS10,S11及びS13に相当している。次に、セッション開設管理処理部124は、適合するエントリがあったという判断に基づきセッション管理処理部122へ、パケット②より後続のパケット③及び④を高優先で転送処理するように、パケット③や④を識別可能なエントリを作成するように依頼する。

【００７８】この依頼時、セッション開設管理処理部124は、受信したパケットのヘッダ内より、プロトコル番号、送信元/宛先IPアドレス、及び送信元/宛先ポート番号を得るとともに、図５(1)に示したセッション開設条件テーブルより優先度を読み出す。そして、セッション開設管理処理部124よりも前段の処理部がセッション開設管理処理部124へパケットと一緒に通知した受信/送信インタフェース番号、及び宛先MACアドレスを得て、これらを同時にセッション管理処理部122へ通知する。

【００７９】このような各処理部間でのデータを通知するとき、前段から後段への通知に関しては、例えばパケットヘッダの更に前に装置内で制御を行うための独自の装置内ヘッダを付加することによって実行する。一方、前段から後段へのデータ通知ではなく、セッション開設管理処理部124からセッション管理処理部122へのデータの通知（後段から前段へのデータ通知）に関しては、セッション開設管理処理部124とセッション管理処理部122との間の信号線125によって実行する。従って、セッション開設管理処理部124からの依頼によって、セッション管理処理部122は、パケット③及び④が識別可能である図６のセッション管理テーブルにおけるセッション管理エントリ901を、ネットワーク管理者が予め作成するのではなく動的に作成する。

【００８０】この手順は、図７のフローチャートにおけるステップS14及びS16に相当しており、プロトコル番号はTCPであるので、ステップS14を経由してステップS16へ移行する処理となる。そして、セッション開設管理処理部124は、上記依頼の確認信号を受理した後、受信パケットをスイッチ部112へ渡す(ステップS17)。スイッチ部112は、受信パケットを、送出インタフェース番号及びそのパケットの優先度に応じて該当するキュー113へ格納し、パケットスケジューリング処理部114が受信パケットをその送出インタフェース115から送出する。

【００８１】パケット③がパケット転送装置100へ到着したとき、LAN1に属する端末群がLAN6に属する端末群へ発信したtelnet通信に関しては、パケット転送装置100は高優先で転送処理するので、パケット③を高優先で転送処理する。すなわち、セッション管理処理部122は、パケット③を受信したならば、セッション管理テーブル123を検索する。この手順は、図8に示すセッション管理処理部122のフローチャートにおけるステップS21及びS21に相当する。

【００８２】セッション管理処理部122が、セッション管理テーブル121を検索しても、セッション開設管理処理部124の依頼に従って、セッション管理処理部122が、作成したセッション管理エントリ901には、パケット③は適合しない（ミスヒット）。これは、上述の如くセッション管理エントリ901をパケット④に適合（ヒット）するように、すなわち端末11～端末62の方向についてだけ適合するように、セッション管理処理部122が作成したからである。

【００８３】したがって、ステップS23を実行し、送信元IPアドレスと宛先IPアドレス、送信元ポート番号と宛先ポート番号、受信インタフェース番号と送信インタフェース番号を入れ替えて、もう一度、セッション管理処理部122がセッション管理テーブル121を検索する（ステップS24）。

【００８４】ここで初めて、パケット③はセッション管理テーブル121に適合することになるので、セッション管理処理部122は、このことを示す反転フラグを立て（ステップS26）、セッション管理エントリ901のタイムスタンプを更新する。このタイムスタンプとは、端末がセッション管理エントリ901のtelnet通信を現在行っているのか否かを、パケット転送装置100が判断するために必要な指標の一つである。

【００８５】なお、ステップS24の検索を行っても、受信パケットが各セッション管理エントリに適合しない場合は、そのまま受信パケットをルーティング処理部107へ送出（ステップS39）することは言うまでも無い。次に、セッション管理処理部122は、セッション管理エントリ901から反転処理を行った後ヒットしたので、受信インタフェース番号及び送信元MACアドレスとして分かる、パケット③の送出インタフェース番号と宛先MACアドレスを、次の処理部であるスイッチ部112へ直接通知する(ステップS27及び S29)。

【００８６】さらに同時に、セッション管理エントリ901から分かる優先度をスイッチ部112へ直接通知する(ステップS30及び S31)。次に、セッション管理処理部122は、telnet通信が終わったときに該当するセッション管理エントリを削除するための処理（後述する）であるステップ(S32～S36)を経て反転フラグを元に戻し(ステップS37)、スイッチ部112への送出インタフェース番号、宛先MACアドレス、及び優先度の通知と同時に、受信パケットをスイッチ部112へ送出する(ステップS38)。

【００８７】なお、セッション管理処理部122からスイッチ部112へパケット及びそのパケットに付随するデー

タを通知するために、上述の如くデータ線126を設けている。セッション管理処理部122が、パケット③に対して、上述のように図8の処理（ステップS29, S34, S36を除く）を実行することによって、パケット転送装置100は、パケット③をスイッチ部112以降で優先転送し、なおかつ、冗長なルーティング処理部107、フィルタリング処理部109、優先制御処理部111、及びセッション開設管理処理部124で実行すべき処理を実行せずに高速にパケット転送処理を実行することができる。

【００８８】さらにパケット④がパケット転送装置100へ到着したとき、LAN1に属する端末群がLAN6に属する端末群へ発信したtelnet通信に関しては、パケット転送装置100は高優先で転送処理するので、パケット転送装置100はパケット④を高優先で転送処理する。このとき、セッション管理処理部122は、一度の検索でセッション管理エントリ901にパケット④が適合するが、このことを除いては、上述のパケット③のときと同様に、図8の処理（ステップS23, S24, S26, S29, S34, S36, S39を除く）を実行する。

【００８９】このように処理を実行することによって、パケット転送装置100は、パケット④をスイッチ部112以降で優先転送し、なおかつ、冗長なルーティング処理部107、フィルタリング処理部109、優先制御処理部111、及びセッション開設管理処理部124で実行する処理を、実行せずに高速にパケット転送処理を実行することができる。

【００９０】次に、図4（1）の時間の流れに沿って、TCP通信の閉鎖時に関してパケット転送装置100が実行する処理を説明する。上記の実施例においては、TCP通信の開設時に関してパケット転送装置100が実行する処理を説明したが、パケット転送装置100は、TCP通信が終了したときも、必要がないエントリをセッション管理テーブル121から削除する等の処理を実行する必要がある。

【００９１】何故なら、図6に示したセッション管理テーブル121には、パケット転送装置100間に跨る端末間の通信が始まる度に、図5に示したセッション開設管理テーブル121のセッション開設条件に応じて、セッション管理処理部122がエントリを動的に追加するので、適切にエントリを削除しないと、パケット転送装置運用中にエントリ数がテーブル121の容量を越えてしまう可能性があるからである。

【００９２】ここで、TCPセッションの閉鎖に関しては、FIN閉鎖（図4(1)）または、RST閉鎖（同図(2)）、またはFIN閉鎖及びRST閉鎖以外の異常終了がある。FIN閉鎖は、端末11と端末62が互いに、TCPパケットヘッダのCTRフラグ（図13（1）参照）がFINであるパケット①及び②を送り合い、これらのFINであるパケット①及び②に対する受信応答パケット(CTRフラグがACK)③を送ることによってセッションを閉鎖する。また、RST閉鎖の場合は、CTRフラグがRSTであるパケット①を端末11または端末62が送ることによって即座にセッションを閉鎖する。

【００９３】FIN閉鎖の場合、TCPパケットヘッダのCTRフラグがFINであるパケット①をパケット転送装置100が受信すると、セッション管理処理部122は、パケット①が適合するセッション管理エントリ901のFINカウンタフィールド値をカウントアップする。この手順は、図８におけるステップS33及びS34に相当する。

【００９４】次に、パケット①を受信した時点では、FINカウンタ=1なので、セッション管理処理部122はステップS35, S37及びS38の順に処理を実行し、受信したパケット①をスイッチ部112へ渡し、スイッチ部112は、パケット①を優先転送する。パケット①は、端末11が発信したパケットであり、端末62は、これを受信して、受信応答パケットを端末11へ送出し、さらにCTRフラグがFINであるパケット②を端末11へ送出する。

【００９５】パケット転送装置100がパケット②を受信すると、セッション管理処理部122は、パケット②が適合するセッション管理エントリ901のFINカウンタフィールド値をカウントアップする。この手順は、ステップS33及びS34に相当する。次に、セッション管理処理部122は、ステップS35を実行し、ここでFINカウンタ=2であるが、CTRフラグはACKではないので、パケット①と同様に、ステップS37及びS38の順に処理を実行する。

【００９６】パケット②を受信した端末11は、端末62へ受信応答パケット③を送信する。パケット転送装置100がパケット③を受信すると、セッション管理処理部122は、ステップS35を実行し、FINカウンタ=2であり、かつパケット③のCTRフラグはACKであるので、パケット③が適合するセッション管理エントリ901を削除する(ステップS36)。

【００９７】このようにセッション管理処理部122が処理を実行することによって、FIN閉鎖の時、TCP通信が終了し、必要のないエントリを削除することができる。したがって、これ以降、パケット転送装置100は、パケット④がLAN6に属する端末群がLAN1に属する端末群へ発信したTCP通信のパケットであるので、パケット④をフィルタリング処理部109によって廃棄する。

【００９８】またRST閉鎖の場合、CTRフラグがRSTであるパケット①を受信したならば、セッション管理処理部122は、パケット①が適合するセッション管理エントリ901を削除する。この手順は、ステップS32及びS36に相当する。したがって、これ以降、パケット転送装置100は、パケット②がLAN6に属する端末群がLAN1に属する端末群へ発信したTCP通信のパケットであるので、パケット②をフィルタリング処理部109によって廃棄する。

【００９９】また、セッションの閉鎖が、上記のような正常な閉鎖ではなく、伝送媒体の断線など異常な終了である場合は、定期的にセキュリティ制御ソフトウェア102または優先制御ソフトウエア103がセッション管理テーブル121の各エントリのタイムスタンプをチェックし、

該ソフトウェアでネットワーク管理者または装置設計者が設定した一定時間を経過した後もパケットの送受信が起きていないエントリは削除する。

【０１００】セッション管理エントリ901のタイムスタンプは、パケット転送装置100が該エントリに適合するパケットを受信する度に、セッション管理処理部122が更新(ステップS25)する。また、上述のようにセキュリティ制御ソフトウェア102または、優先制御ソフトウエア103がセッション管理テーブル121へアクセスするために、ソフトウェア部101からセッション管理テーブル121へ制御線127を設けている。

【０１０１】図9は、使用メモリデバイスとしてCAMを利用する場合の使用メモリ容量を節約したセッション管理テーブル例を示している。CAMは、逐一比較対象となるエントリを読み込み、検索キーと比較するのではなく、各エントリを一度に並列に検索し、各エントリのヒット/ミスヒットを判別することが可能なメモリデバイスなので高速に検索を行うことができるが、1エントリの総ビット長を長くすることはできないという特徴を持つ。

【０１０２】従って、図６に示すように一つのテーブルとしてセッション管理テーブル121を構成した場合、例えば、送信元ポート番号値のみが異なり他のフィールド値が同一であれば、他のフィールド値を一つのエントリとしてインデックスを付けて保有し、該インデックス値と送信元ポート番号の組によってセッション管理テーブルを構成した方が、使用メモリ容量の節約につながる。

【０１０３】IP通信においては、セッション開始するときの宛先ポート番号は、ウェルノウンポートという或る限られた種類のポート番号になる特性があり、またパケット転送装置100を介して送受信されるIPアドレスの組の種類もそのアドレス空間全体と比較して、少ないという特性がある。

【０１０４】そこで、セッション管理テーブルの各フィールドのビット長から考慮して、図9に示すように、CAM-1，CAM-2，CAM-3，CAM-4のように各フィールドを分け、各インデックス値をCAM-5で有することにより、使用メモリ容量を節約したセッション管理テーブルを構築することが好ましい。

【０１０５】図9の実施例では、同図（4）のCAM-4に見られるように、MACアドレスを直接テーブル内に格納するのではなく、MACアドレスを格納している他のテーブルのポインタとして格納した。これは、MACアドレスは、48ビット長と長いので、上述と同様の理由で一つのCAM内への格納は難しいからである。

【０１０６】セッション管理テーブルの検索においては、MACアドレスは、検索を行うキーではなく、どのエントリがヒットするかを判別した後に、ヒットするエントリがあったならば必要となるコンテンツであるので、ポインタで格納することによって、セッション管理テーブルへの検索動作が遅くなることはない。また、MACアドレスを格納している他のテーブルとしては、例えばルーティングテーブル106とがあり、ルーティングテーブル106とMACアドレスの各の領域を共用することも可能である。

【０１０７】上記の実施例では、TCP通信に関して言及したが、次にUDP通信の場合について説明する。図10に示すようなネットワーク構成例において内部ネットワークであるLAN1、LAN2、LAN3に属する端末群が、外部ネットワークであるLAN4、LAN5、LAN6へ発信したUDP通信のアプリケーションの一つであるDNS(Domain Name Service)の通信に関しては許可し、外部ネットワークに属する端末群が内部ネットワークに属する端末群へ発信したUDP通信は許可しないというセキュリティ制御を行うパケット転送装置を、やはり図2に示すような装置構成で実現することができる。

【０１０８】すなわち、図3（2）にはUDP通信の場合におけるセッション開設時のパケットのフローを示しており、図13（2）がUDPのパケットフォーマットを示している。コネクションレス型のUDP通信はコネクション型TCP通信と異なりセッションの開始を示すフラグがパケットヘッダ内に存在しない。したがって、UDP上で通信される個別のアプリケーション毎、すなわちUDPの宛先ポート番号毎にセッションを開始するRequestパケットをパケット転送装置100が識別可能なように、UDPヘッダに続く、アプリケーションデータ部の一部の範囲のビットパターンを、セッション開設管理テーブル121内のUDPセッション開設データテーブル（図5（3））及び対応マスクデータテーブル（同（4））として記憶する。

【０１０９】パケット転送装置100は、受信したUDPパケットに対してセッション開設条件テーブル（同（1））に加えて、このUDPセッション開設データテーブルを検索することによって、受信したUDPパケットが属するUDP通信をセッション管理処理部122が管理すべきか否かを判断する。

【０１１０】セキュリティ制御ソフトウェア102及び優先制御ソフトウエア103が、セッション開設管理テーブル123内のUDPセッション開設データ・テーブルに予めエントリを格納しておく。図3（2）におけるパケット①をパケット転送装置100が受信したときは、外部ネットワークに属する端末群が内部ネットワークに属する端末群へ発信したUDP通信なので、フィルタリング処理部109によってパケット①を廃棄する。

【０１１１】パケット②をパケット転送装置100が受信したときは、セッション開設管理処理部124がセッション開設管理処理テーブル123を検索する。その結果、セキュリティ制御ソフトウェア102が予めセッション開設条件テーブルに作成しておいたプロトコル番号=UDP、宛先ポート番号=53、及び受信インタフェース番号=インタフェースIF1というセッション開設条件エントリ802、または同様に受信インタフェース番号=インタフェースIF2

であるセッション開設条件エントリ803、または同様に受信インタフェース番号=IF3であるセッション開設条件エントリ804の内の、セッション開設条件エントリ806にパケット②がヒットする。これは、図7に示したフローチャート内のステップS12及びS13に相当する。

【０１１２】そして、セッション開設管理処理部124は、プロトコル番号=UDPなので(ステップS14)、UDPセッション開設データテーブルを検索する。その結果、DNSの宛先ポート番号が53であるUDPセッション開設データエントリ806と受信パケットのアプリケーションデータの先頭のビットパターンが適合する(ステップS15)ので、セッション開設管理処理部124は、パケット②をRequestパケットと認識する。

【０１１３】したがって、セッション開設管理処理部124は、上記の実施例と同様にセッション管理処理部122へ、後続のパケット③及び④が認識できるエントリの作成を依頼し(ステップS16)、パケット②をスイッチ部112へ渡す(ステップS17)。パケット③又は④をパケット転送装置100が受信したときも同様に、セッション管理処理部122がパケット③又は④を識別可能なエントリがセッション管理テーブル121にあり、そのエントリには、パケット③又は④を転送するように記述してあるので、これによって、内部ネットワークであるLAN1に属する端末が、外部ネットワークであるLAN6へ発信したDNS通信のパケットである、パケット③又は④をパケット転送装置100は転送することができる。

【０１１４】セッションの閉鎖に関して、コネクションレス型のUDP通信は、上記の実施例のコネクション型TCP通信と違い、通信の終了を示すフラグ等は、UDPヘッダ内に存在しない。UDP通信におけるセッションの閉鎖は、定期的にセキュリティ制御ソフトウェア102または、優先制御ソフトウエア103がセッション管理テーブル121のタイムスタンプをチェックし、該ソフトウェアで設定された一定時間が、経過した後もパケットの送受信が起きていないエントリを削除することよって行うことができる。

【０１１５】

【発明の効果】以上説明したように本発明に係るパケット転送装置によれば、ルーティング処理、フィルタリング処理、及び優先制御処理を実行する主処理部から出力されたパケットがセッション開設条件に適合するか否かを判定し、該パケットについて適合判定した時、該判定部からそのパケット情報を受けて保持し、該パケット情報に基づいて同一セッションに属する後続のパケットを該主処理部のバイパス路に与えるように構成したので、冗長な処理を減じて高速にパケットを転送することが同時にできる効果がある。

【０１１６】また、使用メモリデバイスとしてCAMを使用した場合、各フィールド値のビット長を考慮して、複数のフィールドによって一つのテーブルを構成し、各テーブルエントリに必要な種類数分のインデックス付けし、該インデックスの組み合わせにより、セッション管理テーブルを構成することによって、使用メモリ容量を節約してセッション管理処理ができる効果がある。

【図面の簡単な説明】

【図１】本発明に係るパケット転送装置の処理概念を示したフローチャート図である。

【図２】本発明に係るパケット転送装置の実施例を示すブロック図である。

【図３】セッション開設時のパケットのフローを示した図である。

【図４】セッション閉鎖時のパケットのフローを示した図である。

【図５】本発明に係るパケット転送装置に用いるセッション開設管理テーブルを示した図である。

【図６】本発明に係るパケット転送装置に用いるセッション管理テーブルを示した図である。

【図７】本発明に係るパケット転送装置に用いるセッション開設管理処理部の処理手順を示したフローチャート図である。

【図８】本発明に係るパケット転送装置に用いるセッション管理処理部の処理手順を示したフローチャート図である。

【図９】本発明に係るパケット転送装置の使用メモリ容量を節約したセッション管理テーブル例を示した図である。

【図10】パケット転送装置を含む一般的なネットワーク構成例を示したブロック図である。

【図11】従来のパケット転送装置例を示したブロック図である。

【図12】フィルタリングテーブルを示した図である。

【図13】一般的なパケットのフォーマットを示す図である。

【符号の説明】

1～3, 100 パケット転送装置　11, 12, 13, 2122, 31, 32, 61, 62 端末

101 ソフトウエア部　102セキュリティ制御ソフトウエア

103 優先制御ソフトウエア　104 ハードウエア部

105 受信インタフェース

106 ルーティングテーブル　107 ルーティング処理部

108 フィルタリングテーブル　109 フィルタリング処理部

110 優先制御テーブル　111 優先制御処理部

112 スイッチ部　114パケットスケジューリング処理部

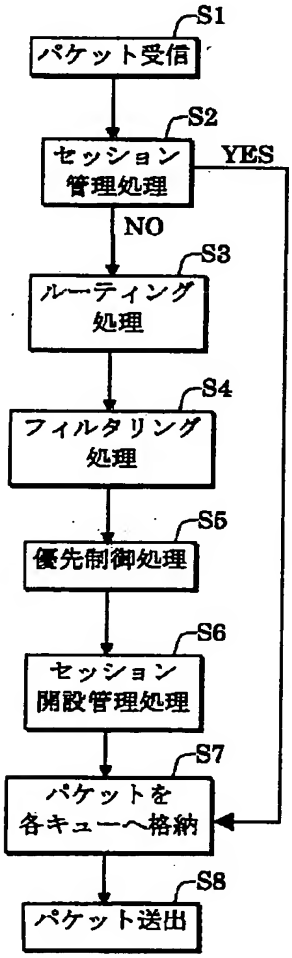
115 送出インタフェース

121セッション管理テーブル　122 セッション管理処理部

123セッション開設管理テーブル　　124　セッショ　　125信号線　　126データ線　　127　制御線
ン開設管理処理部
図中、同一符号は同一又は相当部分を示す。

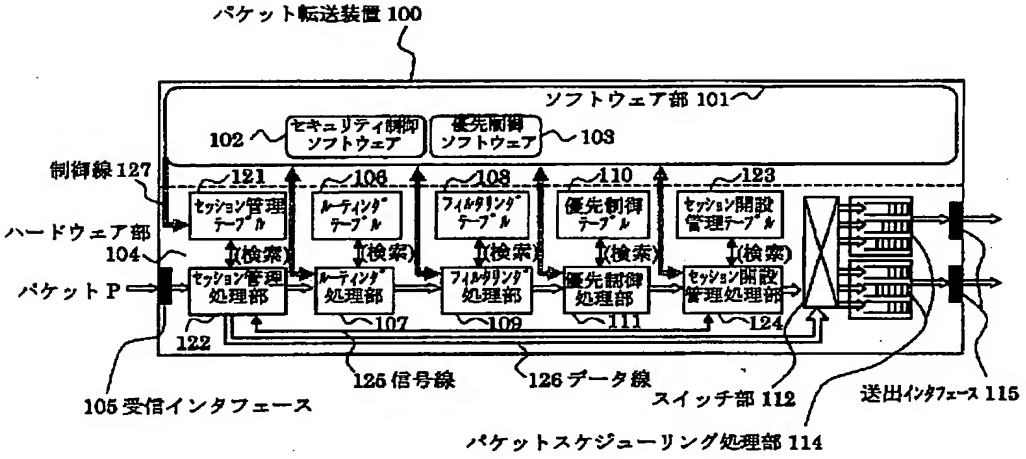
【図１】

パケット転送装置の各処理間のフローチャート



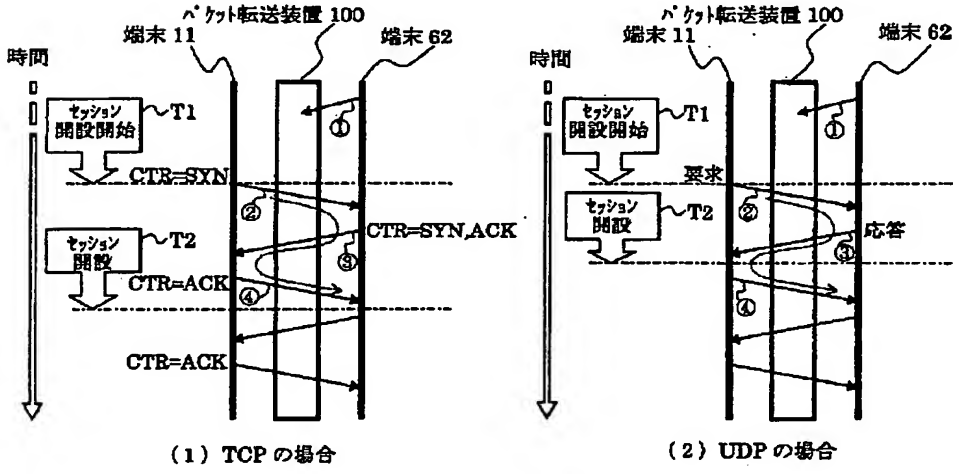
【図２】

本発明の実施例



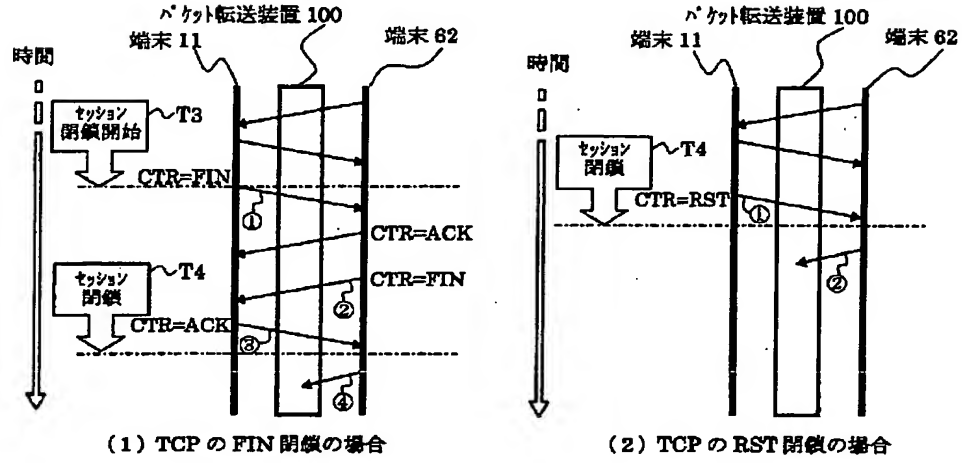
【図３】

セッション開設時のパケットのフロー



【図４】

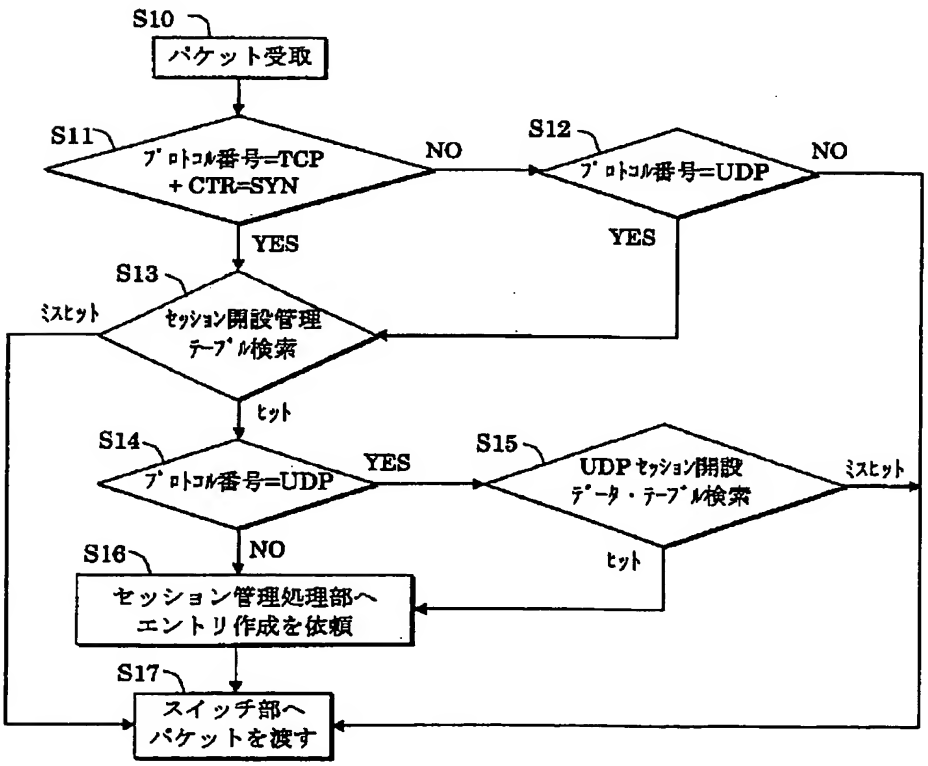
セッション閉鎖時のパケットのフロー



（１）TCP の FIN 閉鎖の場合　　（２）TCP の RST 閉鎖の場合

【図７】

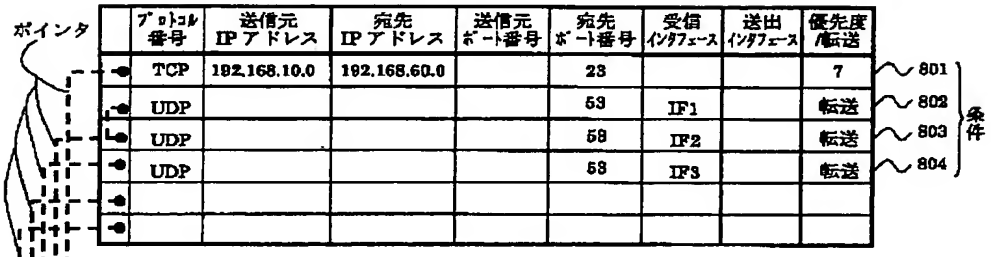
セッション開設管理処理部フローチャート



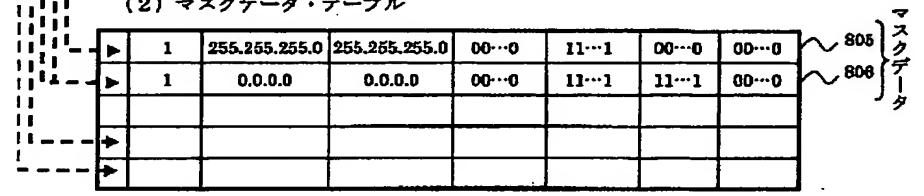
【図５】

セッション開設管理テーブル例

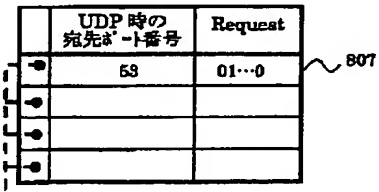
（１）セッション開設条件・テーブル



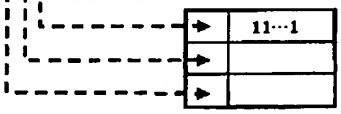
（２）マスクデータ・テーブル



（３）UDPセッション開設データ・テーブル



（４）マスクデータ・テーブル



【図６】

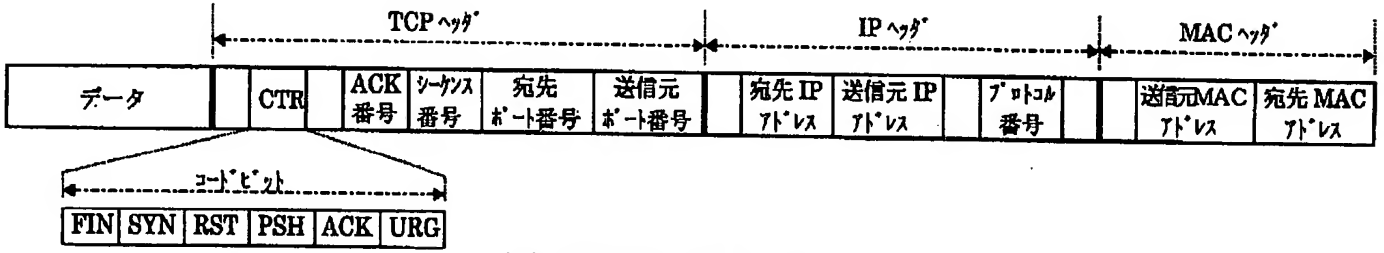
セッション管理テーブル例

ﾌﾟﾛﾄｺﾙ番号	送信元IPアドレス	宛先IPアドレス	送信元ﾎﾟｰﾄ番号	宛先ﾎﾟｰﾄ番号	受信ｲﾝﾀﾌｪｰｽ	送出ｲﾝﾀﾌｪｰｽ	優先度/転送	ﾀｲﾑｽﾀﾝﾌﾟ	FINｶｳﾝﾀ	宛先MACｱﾄﾞﾚｽ	送信元MACｱﾄﾞﾚｽ
TCP	192.168.10.1	192.168.60.2	1023	23	IF1	IF4	7	0	0	00:00:…:52	00:00:…:c0

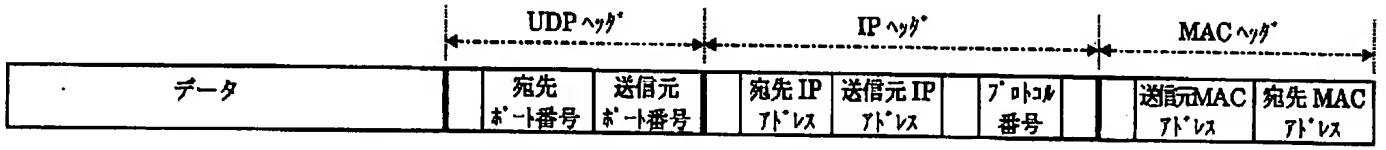
901

【図１３】

ＩＰパケットフォーマット



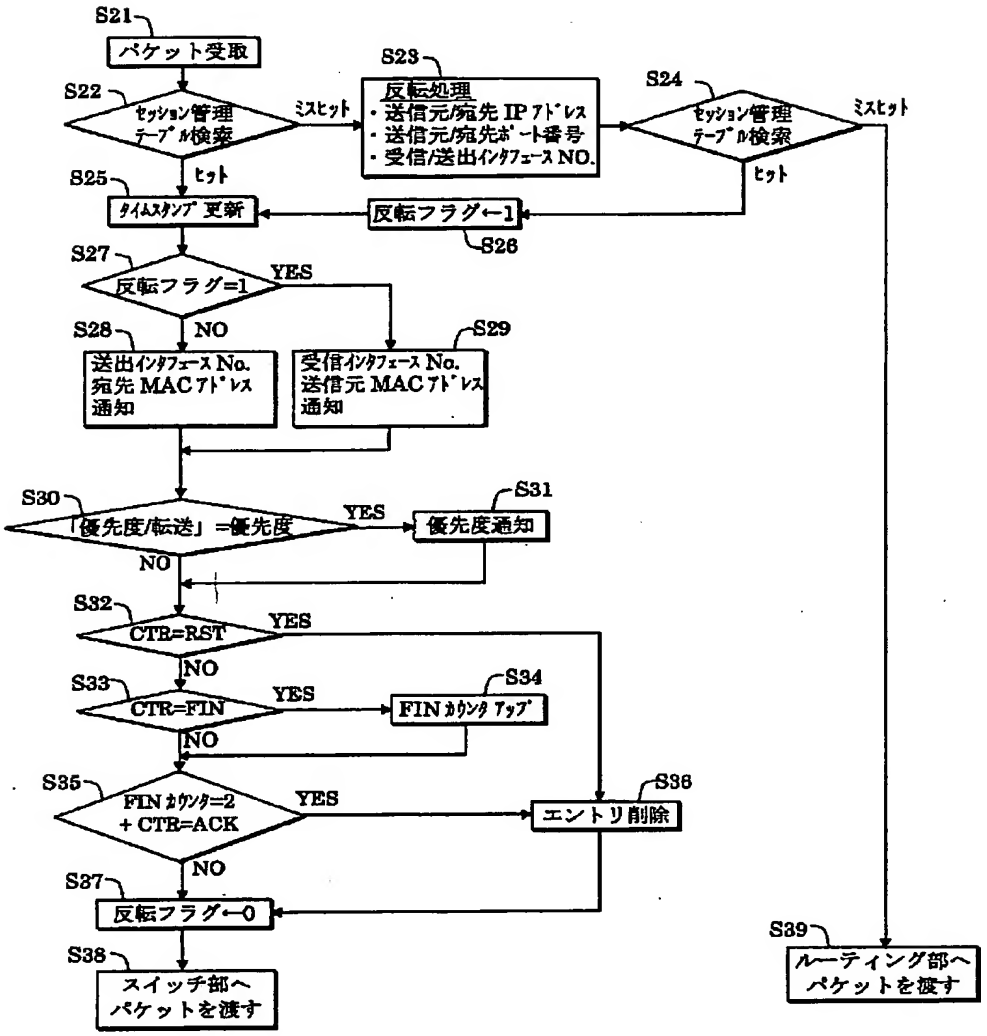
（1）TCPパケットフォーマット



（2）UDPパケットフォーマット

【図８】

セッション管理処理部のフローチャート



【図９】

使用メモリ容量を節約したセッション管理テーブル例

（1）CAM-1

インデックス 1	プロトコル番号	宛先ポート番号	受信インタフェース	送出インタフェース

（2）CAM-2

インデックス 2	送信元IPアドレス

（3）CAM-3

インデックス 3	宛先IPアドレス

（4）CAM-4

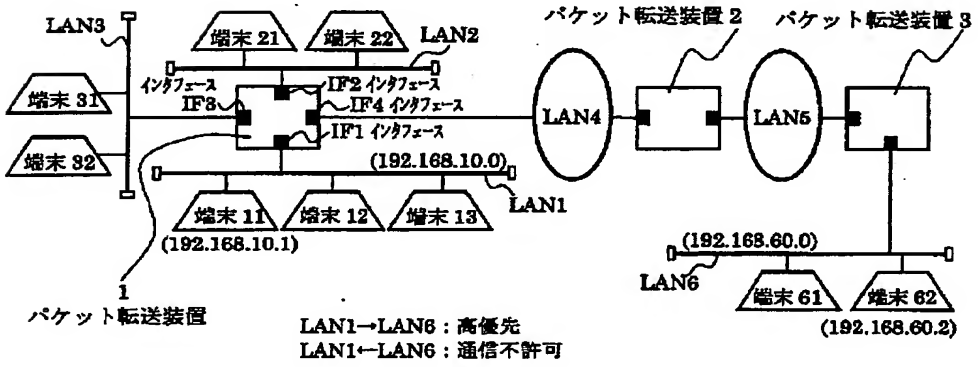
インデックス 4	送信元ポート番号	優先度/転送	タイムスタンプ	FINカウンタ	宛先MACアドレス・ポインタ	送信元MACアドレス・ポインタ

（5）CAM-5

インデックス 1	インデックス 2	インデックス 3	インデックス 4

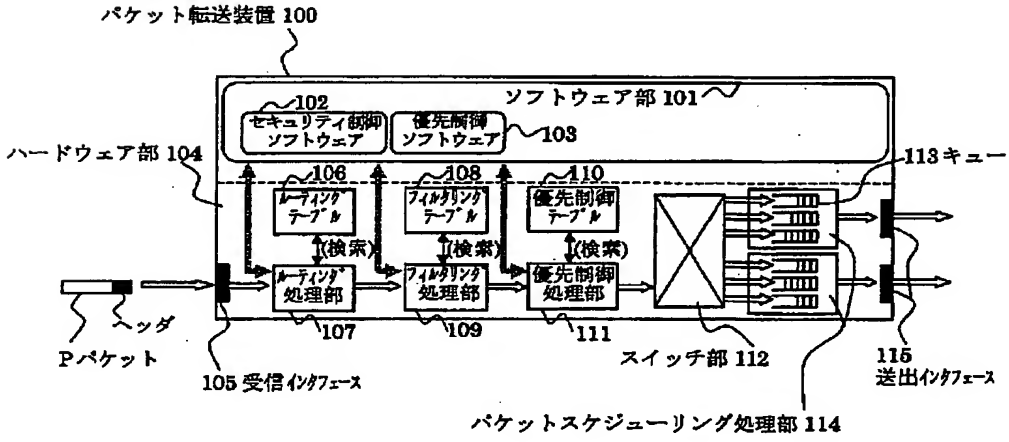
【図１０】

パケット転送装置を含むネットワーク構成例



【図１１】

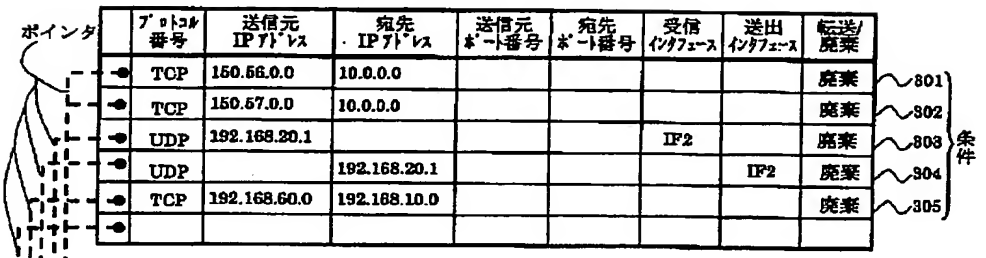
従来例



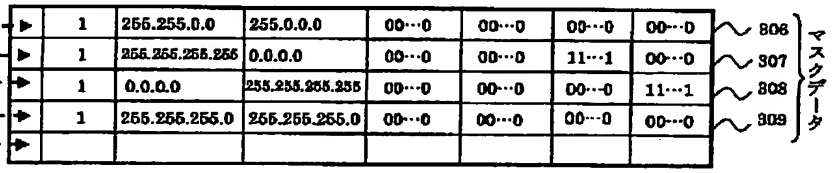
【図１２】

フィルタリングテーブル例

（１）フィルタリング条件・テーブル



（２）マスクデータ・テーブル



フロントページの続き

Ｆターム(参考) 5K030 GA01 GA06 GA15 HA08 HB16
HB28 HD06 KA05 KX18 KX24
KX29 LB03 LB05 LE05
5K034 AA01 AA11 DD03 EE11 FF11
FF13 KK29 LL02 MM11 MM21
9A001 CC06 CC07 CC08 DD10 JJ18
JJ25 KK56